

In re Patent Application of

Atty LSN-36-1522
Dkt.

EVANS et al

C# M#

Serial No. 10/049,844

TC/A.U. 2132

Filed: February 19, 2002

Examiner: L. Lashley

Date: August 17, 2007

Title: PACKET AUTHENTICATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REQUEST FOR RECONSIDERATION

This is a response/amendment/letter in the above-identified application and includes an attachment which is hereby incorporated by reference and the signature below serves as the signature to the attachment in the absence of any other signature thereon.

☐ **Correspondence Address Indication Form Attached.****Fees are attached as calculated below:**

Total effective claims after amendment	0	minus highest number	
previously paid for	20	(at least 20) =	0 x \$50.00
			\$0.00 (1202)/\$0.00 (2202) \$

Independent claims after amendment	0	minus highest number	
previously paid for	3	(at least 3) =	0 x \$200.00
			\$0.00 (1201)/\$0.00 (2201) \$

If proper multiple dependent claims now added for first time, (ignore improper); add
\$360.00 (1203)/\$180.00 (2203) \$

Petition is hereby made to extend the current due date so as to cover the filing date of this
paper and attachment(s)

One Month Extension	\$120.00 (1251)/\$60.00 (2251)
Two Month Extensions	\$450.00 (1252)/\$225.00 (2252)
Three Month Extensions	\$1020.00 (1253)/\$510.00 (2253)
Four Month Extensions	\$1590.00 (1254)/\$795.00 (2254)
Five Month Extensions	\$2160.00 (1255)/\$1080.00 (2255) \$

Terminal disclaimer enclosed, add
\$130.00 (1814)/\$65.00 (2814) \$

☐ Applicant claims "small entity" status. ☐ Statement filed herewith

Rule 56 Information Disclosure Statement Filing Fee	\$180.00 (1806)	\$	0.00
---	-----------------	----	------

Assignment Recording Fee	\$40.00 (8021)	\$	0.00
--------------------------	----------------	----	------

Other:		\$	0.00
--------	--	----	------

TOTAL FEE	\$	0.00
------------------	-----------	-------------

☐ **CREDIT CARD PAYMENT FORM ATTACHED.**

The Commissioner is hereby authorized to charge any deficiency, or credit any overpayment, in the fee(s) filed, or asserted to be filed, or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Account No. 14-1140. A duplicate copy of this sheet is attached.

901 North Glebe Road, 11th Floor
Arlington, Virginia 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100
LSN:vc

NIXON & VANDERHYTE P.C.
By Atty: Larry S. Nixon, Reg. No. 25,640

Signature: Larry S. Nixon



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of

EVANS et al

Atty. Ref.: 36-1522; Confirmation No. 6117

Appl. No. 10/049,844

TC/A.U. 2132

Filed: February 19, 2002

Examiner: L. Lashley

For: PACKET AUTHENTICATION

* * * * *

August 17, 2007

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

REQUEST FOR RECONSIDERATION

In response to the Office Action dated 05/17/2007, reconsideration of this application is requested in light of the following comments.

The rejection of claims 1-2, 4-6, 10-16 and 19-21 under 35 U.S.C. §103 as allegedly being made “obvious” based on Naslund ‘676 in view of McDonald ‘827 is respectfully traversed.

Naslund describes a method for authenticating the identity of a mobile station. The method is designed to operate within the AMPS standard for mobile communication, a standard that imposes certain restrictions on what can be transmitted over the air interface between a mobile station and the network. Naslund is designed to operate

within this AMPS standard without any modification to the standard, and does so by utilizing the existing data fields defined in the standard. More specifically, the equipment serial number (ESN) data field is encrypted and located within the same data field as the unencrypted ESN thereby avoiding any changes to the AMPS standard (see 2:26-32).

Naslund describes a way of utilizing a COUNT variable to encrypt the ESN. The COUNT variable is maintained at the mobile station and in the network (see 3:62-4:5). The COUNT variable is used to modify (effectively encrypt) the ESN to create a modified ESN or MESN (see 4:26-34) by the mobile station. The MESN is then sent in place of the ESN by the mobile station (4:49-52), and a corresponding calculation is performed at the receiver based on the COUNT variable stored at the receiver. If the MESN received from the mobile station matches that of MESN as generated locally by the receiver, then the mobile station is verified by the receiver and access is granted to the network (4:53-61). This is summarized in 4:8-14, and 6:51-62.

An alternative method is described by Naslund in the text referred to by the Examiner (7:5-7). This alternative method suggests using indexed random numbers in place of counters for the COUNT variable, which can be supplied to the mobile station and system in advance.

However, this alternative method, and indeed the main method summarized above, fails to disclose the features of steps (iii) and (iv) of claim 1 as the Examiner already recognizes. McDonald does not supply these admitted deficiencies.

McDonald describes a method of using a secret key/cipher that is applied to messages to generate an authentication code or authenticator, which can be sent with the message itself (1:64 to 2:2). The authenticator effectively works as a digital signature for authenticating the identity of the sender. The examiner has referred to Figure 2, which is described in more detail from 4:39 onwards and relates to an alternative method that can prevent further types of attack. While Figure 2 and the corresponding text do refer to the use of a random number, this random number is still not chosen from any "list of stored random numbers" that has been previously shared, nor is the random number selected restricted to one "that has not previously been selected and included in a data packet to be sent", both as required in step (iii) of claim 1.

Furthermore, contrary to the Examiner's suggestion, these two prior art references would not be combined by a skilled person.

First, the teachings in the two references are not compatible. Naslund relates to a system that is designed to operate within the specific restrictions imposed by the AMPS standard. This means that the starting point, and indeed the entire teaching and motivation of Naslund, are restricted to re-use of existing data fields within AMPS, which in the described solution is done by encrypting the ESN field. The teachings in Naslund thus force a skilled person to limit any modifications to re-use of existing fields such as the ESN field. This is incompatible with selecting a random number selected from a stored list where the random number has not previously been selected, and including the random number in a data packet (step (iii) of claim 1). The inclusion of the

random number in a data packet as required by claim 1 is incompatible with the teachings in Naslund, where there is no room for additional data to be sent given the strict standard requirements that the teachings in Naslund must adhere to.

Second, there is also no motivation for a skilled person reading Naslund to modify that system as suggested by the Examiner. The solution set out in Naslund by itself already solves the problem of attaining a high degree of security and minimizes the risk of fraudulent transmission of data packets as suggested by the Examiner. Indeed, the solution is arguably even more effective than the argued combination and thus there is even less motivation to modify the solution further, and in a manner than would go against the teachings and requirements set out within Naslund.

Therefore, the cited references fail to disclose all features of claim 1, whether taken individually or in combination. The features in claim 1 are tightly interlinked and are not simply a mosaic of several features that can be found individually in the prior art, which is what the examiner seems to be suggesting with casual references to very general portions of text and a Figure (see single reference to Figure 2 of Naslund for many of the key features in claim 1) as basis for the rejection.

Perhaps the Examiner has misunderstood claim 2. Claim 2 relates to how the recipient server sends back an acknowledge message with a sequence number, where the sequence number corresponds to the position of the received random number in the stored list of random numbers. The sequence number is verified by the first sever

to verify the authenticity of the recipient. If the sequence number is incorrect, then the data packet is resent. This is described on page 10, lines 11-27 of the specification.

The Naslund text referenced by the Examiner does not teach such an arrangement. The text referenced by the examiner relates to how a new MESN can be calculated. There is no discussion of sending any acknowledgement message with a sequence number. Only the use of a new COUNT variable to calculate MESN and comparing the received MESN with the newly calculated MESN is described here. It is clear that only the original MESN is ever sent, not some sequence number corresponding to a position in a list as claimed.

Comments given above with respect to claims 1 and 2 are also believed to apply to claims 4 and 5 respectively. Similarly, those arguments are also believed to apply to claims 6 and 7 respectively. Yet further, those same arguments apply to claims 10 and 11 respectively.

While independent claim 12 does not require the unique data values stored in the first and other server to be random (dependent claims 13 et seq. do however), many other features already noted above with respect to claim 1 do still apply to independent claim 12 and are not found in the cited art. Dependent claims 16 and 17 also require use of the position of the selected data value in the list, etc. and are thus analogous to the discussion given above for claim 2.

Given these fundamental deficiencies with respect to the above discussed features of the independent claims (and some dependent claims), it is not believed necessary at

EVANS et al
Appl. No. 10/049,844
August 17, 2007

this time to detail the additional deficiencies of the cited references with respect to other features of these or other claims.

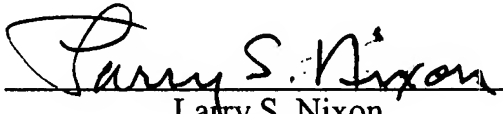
The rejection of claims 3, 7-9, and 17-18 under 35 U.S.C. §103 as being made "obvious" based on Naslund/McDonald in further view of Nishio '732 is also respectfully traversed.

Fundamental deficiencies of Naslund and McDonald have already been noted above with respect to parent claims. Nishio does not supply those deficiencies.

Accordingly, it is not believed necessary at this time to explain the further deficiencies of this allegedly "obvious" combination of references with respect to the additional features

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: 
Larry S. Nixon
Reg. No. 25,640

LSN:vc
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100